REMARKS

Claim 59 has been amended. Claims 1-67 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 102(e) Rejection:

The Examiner rejected claims 1, 4-10, 19, 21-26, 36, 38-42, 48, 52-60, 62, 66 and 67 as being anticipated by Chen et al. (U.S. Patent 6,763,365) (hereinafter "Chen"). Applicants traverse this rejection for at least the following reasons.

Regarding claim 1, contrary to the Examiner's assertion, Chen fails to disclose *a first arithmetic circuit comprising a first plurality of arithmetic structures feeding back high order bits of a previously executed arithmetic instruction in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures.* The Examiner's submits that these limitations are taught in col. 11, lines 34-40 (noting only, "feedback; first using circuit; then using circuit again with register provided with output from first operational stage"), and col. 10, lines 13-26 (noting only, "multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A, B").

Applicants assert that the cited passages do not disclose the above-referenced limitations. For example, nothing in the cited passages describes a first circuit *feeding back high order bits of a previously executed arithmetic instruction* to a second circuit, much less to a second circuit that is currently executing a different arithmetic instruction, as recited in a subsequent limitation of claim 1. Instead, the "multiplication with feedback" described therein appears to refer to feedback provided between operational stages of Chen's system while executing a single multiplication instruction. For example, the cited passage in col. 11 describes the multiplication operation "AB mod N." In Chen, a hardware circuit may execute this single multiplication operation in two phases.

However, there is no feedback of a partial result from a previously executed single arithmetic instruction (i.e., a different instruction) described. The Examiner's citation in col. 10 describes the operation of Chen's hardware circuit in more detail, but also does not disclose feedback of a partial result from a previously executed single arithmetic instruction, as required by Applicants' claim.

Further regarding claim 1, Chen fails to disclose *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction in the public-key cryptography application, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit; storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application.*

The Examiner submits that this entire collection of limitations is taught in col. 4, lines 8-11 (noting only, "multiplication and addition are performed by large circuits"); in col. 10, lines 13-36 (without including any remarks regarding this passage); and in col. 11, lines 34-40 (noting only, "feedback; first using circuit; then using circuit again with register provided with output from first operational stage (multiplication with feedback)").

Applicants assert that the Examiner has failed to fully and clearly state his ground of rejection of claim 1 and has therefore failed to establish a *prima facie* case of anticipation given that the burden of proof falls on the Office. The Examiner's remarks (quoted above) refer only generally to features that he believes are taught by the cited passages of Chen without describing how he believes these passages (or elements described therein) disclose each of the above-referenced limitations of claim 1. Since the features noted by the Examiner do not correspond to the language recited in the above-referenced claim limitations, it is not clear or how he interprets the cited passages to teach the specific limitations of claim 1 as arranged in the claim**.** The statute clearly places the burden of proof on the Patent Office to prove a *prima facie* rejection. *In re Warner*, 154 USPQ 173, 177 (C.C.P.A. 1967), *cert. denied*, 389 U.S. 1057 (1968). The Examiner's vague assertions, which lack a clear mapping between the teachings of Chen and Applicants' claim, cannot be said to establish a *prima facie* case of anticipation.

In addition, the cited passages do not disclose all of the above-referenced limitations. For example, these passage do not describe *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction*, i.e., a different arithmetic instruction than the *previously executed arithmetic instruction* recited in claim 1. As noted above, Chen does not describe the execution of two different arithmetic instructions in the manner recited in Applicants' claim.

Chen also fails to disclose *the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit.* The Examiner's general reference to "multiplication with feedback" and a description of a hardware circuit usable to execute a single multiplication instruction clearly do not teach these specific limitations of claim 1.

Applicants further assert that the cited passages clearly do not disclose *storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application.* These passages do not describe anything about storing a partial result, or using the stored partial result in a subsequent computation in a public-key cryptography application. Instead, they describe the execution of a single multiplication instruction.

As discussed above, the descriptions of individual features listed by the Examiner do not teach the specific combination of limitations recited in claim 1, as arranged in the claim. The Examiner is clearly attempting a piecemeal reconstruction of Applicants' invention in hindsight without consider the claimed invention as a whole. Such reconstruction is improper. *See, e.g., Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985). For example, a general reference to "multiplication with feedback" and a description of a hardware circuit usable to execute a single multiplication instruction clearly do not teach the specific limitations recited in claim 1 regarding *feeding back high order bits of a previously executed arithmetic instruction... to a second arithmetic circuit*, and *the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number.* In another example, the Examiner's statement that "multiplication and addition are performed by large circuits" teaches nothing about the limitations recited in claim 1.

Anticipation requires the presence in a single prior art reference disclosure of each and every limitation of the claimed invention, **arranged as in the claim**. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The **identical invention must** be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). **As discussed above, Chen clearly fails to disclose all the limitations of claim 1, as arranged in the claim**.

For at least the reasons above, Chen cannot be said to anticipate claim 1 and removal of the rejection there is respectfully requested.

Independent claims 38 and 66 include limitations similar to those recited in claim 1 and discussed above, and were rejected for similar reasons. Therefore, the arguments presented above apply with equal force to these claims, as well.

Independent claim 21 includes limitations similar to those recited in claim 1 and discussed above, and was rejected for reasons similar to those discussed above regarding claim 1. In fact, the Examiner includes several of the same citations and notes several of the same features of Chen in rejecting claim 21. Therefore, Applicants traverse the rejection of this claim for at least the reasons presented above regarding limitations in this claim that are similar to those in claim 1.

In addition, claim 21 recites *supplying a third number to the second arithmetic circuit* and *the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number and with the third number*. **Applicants note that the Examiner does not include any additional remarks regarding this limitation or any additional citations in the reference to teach it.** Therefore, the Examiner has failed to state a *prima facie* rejection of claim 21. Applicants assert that the Examiner's citations and remarks regarding "multiplication and addition are performed by large circuits," "multiplication with feedback," and "arithmetic operations to support acceleration of cryptographic functions" clearly teach nothing about these limitations of claim 21. In addition, nothing in the cited passages describes <u>a third number</u> being supplied to any of the arithmetic circuits, much less one that is added to high order bits of a previously executed arithmetic instruction and low order bits of a result of a multiplication to produce a partial result, as in claim 21.

For at least the reasons above, Chen cannot be said to anticipate claim 21 and removal of the rejection thereof is respectfully requested.

Claims 53 and 67 include limitations similar to those recited in claims 1 and 21 and discussed above, and were rejected for the same reasons as claims 1 and 21. Therefore, the arguments presented above apply with equal force to these claims, as well.

<u>Section 103(a) Rejection</u>:

The Examiner rejected claims 2, 3, 15-18, 27-29, 35 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Chen in view of Lasher et al. (U.S. Patent 4,863,247) (hereinafter “Lasher”), claims 11, 20, 30, 31, 37, 47 and 61 as being unpatentable over Chen in view of Stribaek et al. (U.S. Patent 7,181,484) (hereinafter “Stribaek”), claims 12-14, 32-34, 49-51 and 63-65 as being unpatentable over Chen, et al. (U.S. Patent 6,687,725) (hereinafter “Chen2”).

In regard to the rejections under both § 102(e) and § 103(a), Applicants assert that numerous ones of the dependent claims recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a discussion of the dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-31500/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: September 12, 2008